IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of: James Malcolm Vignoles et al.

Application No.: 09/938,489   Group No.: 2137
Filed: August 27, 2001   Examiner: Pyzocha, M.
For: UPDATE STATUS ALERTING FOR A MALWARE SCANNER

Mail Stop Appeal Briefs – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

TRANSMITTAL OF APPEAL BRIEF
(PATENT APPLICATION--37 C.F.R. § 41.37)

1.   This brief is in furtherance of the Notice of Appeal, filed in this case on 03/09/2007, and in response to the decision on the Petition for Withdrawal of Abandonment, mailed 09/19/2008.

2.   STATUS OF APPLICANT

      This application is on behalf of other than a small entity.

3.   FEE FOR FILING APPEAL BRIEF

      Pursuant to 37 C.F.R. § 41.20(b)(2), the fee for filing the Appeal Brief is:

      other than a small entity $540.00

                      Appeal Brief fee due   **$540.00**

4.   EXTENSION OF TERM

      The proceedings herein are for a patent application and the provisions of 37 C.F.R. § 1.136 apply.

      Applicant believes that no extension of term is required. However, this conditional petition is being made to provide for the possibility that applicant has inadvertently overlooked the need for a petition and fee for extension of time.

5.   TOTAL FEE DUE

      The total fee due is:

      Appeal brief fee $540.00
      Extension fee (if any) $0.00

                      TOTAL FEE DUE   **$540.00**

6.   FEE PAYMENT

Authorization is hereby made to charge the amount of $540.00 to Deposit Account No. 50-1351 (Order No. NAHP495).

7.   FEE DEFICIENCY

If any additional extension and/or fee is required, and if any additional fee for claims is required, charge Deposit Account No. 50-1351 (Order No. NAHP495).

Date: November 19, 2008   /KEVINZILKA/

                                      Signature of Practitioner

Reg. No.: 41,429   Kevin J. Zilka

Tel. No.: 408-971-2573   Zilka-Kotab, PC

Customer No.: 28875   P.O. Box 721120

                                       San Jose, CA 95172-1120

<div align="right">**PATENT**</div>

In re application of:	)
	)
Vignoles et al.	) Group Art Unit: 2137
	)
Application No. 09/938,489	) Examiner: Pyzocha, Michael J.
	)
Filed: 08/27/2001	) Atty. Docket No.
	) NAI1P495/01.018.01
For: UPDATE STATUS ALTERING FOR A	)
MALWARE SCANNER	) Date: 11/19/2008
	)
	)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

ATTENTION: Board of Patent Appeals and Interferences

APPEAL BRIEF (37 C.F.R. § 41.37)

This brief is in furtherance of the Notice of Appeal, filed in this case on 03/09/2007, and in response to the decision on the Petition for Withdrawal of Abandonment, mailed 09/19/2008.

The fees required under § 1.17, and any required petition for extension of time for filing this brief and fees therefor, are dealt with in the accompanying TRANSMITTAL OF APPEAL BRIEF.

This brief contains these items under the following headings, and in the order set forth below (37 C.F.R. § 41.37(c)(i)):

I	REAL PARTY IN INTEREST
II	RELATED APPEALS AND INTERFERENCES
III	STATUS OF CLAIMS
IV	STATUS OF AMENDMENTS
V	SUMMARY OF CLAIMED SUBJECT MATTER

The final page of this brief bears the practitioner's signature.

I REAL PARTY IN INTEREST (37 C.F.R. § 41.37(c)(1)(i))

The real party in interest in this appeal is McAfee, Inc.

II RELATED APPEALS AND INTERFERENCES (37 C.F.R. § 41.37(c) (1)(ii))

With respect to other prior or pending appeals, interferences, or related judicial proceedings that will directly affect, or be directly affected by, or have a bearing on the Board's decision in the pending appeal, there are no other such appeals, interferences, or related judicial proceedings.

A Related Proceedings Appendix is appended hereto.

III STATUS OF CLAIMS (37 C.F.R. § 41.37(c) (1)(iii))

A.   TOTAL NUMBER OF CLAIMS IN APPLICATION

Claims in the application are: 1, 2, 9-14, 21-26, and 33-37

B.   STATUS OF ALL THE CLAIMS IN APPLICATION

1.   Claims withdrawn from consideration: None
2.   Claims pending: 1, 2, 9-14, 21-26, and 33-37
3.   Claims allowed: None
4.   Claims rejected: 1, 2, 9-14, 21-26, and 33-37
5.   Claims cancelled: 3-8, 15-20, and 27-32

C.   CLAIMS ON APPEAL

The claims on appeal are: 1, 2, 9-14, 21-26, and 33-37

See additional status information in the Appendix of Claims.

IV STATUS OF AMENDMENTS (37 C.F.R. § 41.37(c)(1)(iv))

As to the status of any amendment filed subsequent to final rejection, the Amendment submitted on 10/12/2005 was not entered by the Examiner, and the Amendment submitted on 07/24/2006 was entered by the Examiner.

V SUMMARY OF CLAIMED SUBJECT MATTER (37 C.F.R. § 41.37(c)(1)(v))

With respect to a summary of Claim 1, as shown in Figures 2, 4, 5, and 6 et al., a computer program product embodied on a tangible computer readable medium is provided that is operable to control a computer (e.g. see item 200 of Figure 6, etc.) to issue an alert for an out-of-date update status of a malware scanner. The computer program product comprises (i) reading logic that is operable to read an update status field (e.g. see item 66 of Figure 4, etc.) associated with a computer file (e.g. see item 34 of Figure 2, item 70 of Figure 4, item 74 of Figure 5, etc.) to be scanned by a current malware scanner, where the update status field is indicative of an update status of a previous malware scanner that has scanned the computer file and associated the update status field with the computer file.   Additionally, the computer program product comprises (ii) comparison logic that is operable to compare the update status of the previous malware scanner with an update status of the current malware scanner, as well as (iii) alert issuing logic that is operable if the update status of the current malware scanner does not match the update status of the previous malware scanner to issue an update status alert indicative of an out-of-date update status for whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status.

Further, the computer program product comprises (iv) change logging logic that is operable to log changes to the update status field to create a change history in an update status tracking database (e.g. see item 46 of Figure 2, etc.) to enable identification of weaknesses within update status management based on the change history. Further still, if the current malware scanner has a less out-of-date update status than the previous malware scanner, then the update status field associated with the computer file is changed to correspond to the current malware scanner. Also, the update status alert includes one or more of (i) a user alert that is issued on whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status, and (ii) an administrator alert that is issued to an administrator of whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status.

In addition, if there is no the update status associated with the computer file at a first malware scanning, then the update status field is generated and associated with the computer file, and the update status tracking database is updated. Furthermore, the update status field is included

within an update status file (e.g. see item 36 of Figure 2, item 68 of Figure 4, etc.) passed together and associated with the computer file between malware scanners. Further still, the update status file and the computer file are combined into a combined file (e.g. see item 38 of Figure 2, item 72 of Figure 4, etc.) that is passed as a single entity between the malware scanners, and the combined file is a file compressed combination of the update status file and the computer file. See, for example, Page 3, lines 11-24 and 34; Page 4, lines 1-2, 12-16, and 18-24; and Page 9, lines 25-28 et al.

With respect to a summary of Claim 13, as shown in Figures 2, 4, 5, and 6 et al., a computer-implemented method performed with computer code embodied on a tangible computer readable medium is provided for alerting an out-of-date update status of a malware scanner. In use, an update status field (e.g. see item 66 of Figure 4, etc.) associated with a computer file (e.g. see item 34 of Figure 2, item 70 of Figure 4, item 74 of Figure 5, etc.) to be scanned by a current malware scanner is read, where the update status field is indicative of an update status of a previous malware scanner that has scanned the computer file and associated the update status field with the computer file. Additionally, the update status of the previous malware scanner is compared with an update status of the current malware scanner. Further, if the update status of the current malware scanner does not match the update status of the previous malware scanner, then an update status alert indicative of an out-of-date update status is issued for whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status.

Further still, changes to the update status field are logged to create a change history in an update status tracking database (e.g. see item 46 of Figure 2, etc.) to enable identification of weaknesses within update status management based on the change history. Also, if the current malware scanner has a less out-of-date update status than the previous malware scanner, then the update status field associated with the computer file is changed to correspond to the current malware scanner. Additionally, the update status alert includes one or more of (i) a user alert that is issued on whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status, and (ii) an administrator alert that is issued to an administrator of whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status.

In addition, if there is no the update status associated with the computer file at a first malware scanning, then the update status field is generated and associated with the computer file, and the update status tracking database is updated. Furthermore, the update status field is included within an update status file (e.g. see item 36 of Figure 2, item 68 of Figure 4, etc.) passed together and associated with the computer file between malware scanners. Further still, the update status file and the computer file are combined into a combined file (e.g. see item 38 of Figure 2, item 72 of Figure 4, etc.) that is passed as a single entity between the malware scanners, and the combined file is a file compressed combination of the update status file and the computer file. See, for example, Page 3, line 34; Page 4, lines 1-2, 12-16, and 18-24; Page 5, lines 11-23; and Page 9, lines 25-28 et al.

With respect to a summary of Claim 25, as shown in Figures 2, 4, 5, and 6 et al., an apparatus including a tangible computer readable medium is provided for issuing an alert for an out-of-date update status of a malware scanner. The apparatus comprises (i) a reader that is operable to read an update status field (e.g. see item 66 of Figure 4, etc.) associated with a computer file (e.g. see item 34 of Figure 2, item 70 of Figure 4, item 74 of Figure 5, etc.) to be scanned by a current malware scanner, where the update status field is indicative of an update status of a previous malware scanner that has scanned the computer file and associated the update status field with the computer file. Additionally, the apparatus comprises (ii) a comparitor that is operable to compare the update status of the previous malware scanner with an update status of the current malware scanner. Further, the apparatus comprises (iii) an alert issuer that is operable if the update status of the current malware scanner does not match the update status of the previous malware scanner to issue an update status alert that is indicative of an out-of-date update status for whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status.

Further still, the apparatus comprises (iv) a change logger that is operable to log changes to the update status field to create a change history in an update status tracking database (e.g. see item 46 of Figure 2, etc.) to enable identification of weaknesses within update status management based on the change history. Also, if the current malware scanner has a less out-of-date update status than the previous malware scanner, then the update status field associated with the

computer file is changed to correspond to the current malware scanner. Additionally, the update status alert includes one or more of (i) a user alert that is issued on whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status, and (ii) an administrator alert that is issued to an administrator of whichever one of the current malware scanner and the previous malware scanner has a most out-of-date update status.

In addition, if there is no the update status associated with the computer file at a first malware scanning, then the update status field is generated and associated with the computer file, and the update status tracking database is updated. Furthermore, the update status field is included within an update status file (e.g. see item 36 of Figure 2, item 68 of Figure 4, etc.) passed together and associated with the computer file between malware scanners. Further still, the update status file and the computer file are combined into a combined file (e.g. see item 38 of Figure 2, item 72 of Figure 4, etc.) that is passed as a single entity between the malware scanners, and the combined file is a file compressed combination of the update status file and the computer file. See, for example, Page 3, line 34; Page 4, lines 1-2, 12-16, and 18-24; Page 5, line 25-Page 6, line 3; and Page 9, lines 25-28 et al.

Of course, the above citations are merely examples of the above claim language and should not be construed as limiting in any manner.

VI GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL (37 C.F.R. § 41.37(c)(1)(vi))

Following, under each issue listed, is a concise statement setting forth the corresponding ground of rejection.

Issue # 1: The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

Issue # 2: The Examiner has rejected Claims 1-2, 9-14, 21-26, and 33-37 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

Issue # 3: The Examiner has rejected Claims 1-2, 9-14, 21-26, and 33-37 under 35 U.S.C. 101 as being directed towards non-statutory subject matter.

VII ARGUMENT (37 C.F.R. § 41.37(c)(1)(vii))

The claims of the groups noted below do not stand or fall together. In the present section, appellant explains why the claims of each group are believed to be separately patentable.

Issue # 1:

The Examiner has objected to the specification as failing to provide proper antecedent basis for the claimed subject matter.

Specifically, the Examiner has asserted that "[e]ach independent claim has been amended to include at least the phrase 'tangible computer readable medium'" and that "nowhere in the specification is this phrase disclosed." Appellant disagrees and respectfully asserts that Page 11, lines 13-15 of the specification discloses "computer program instructions that may be stored in one or more of the <u>random access memory</u> 204, the <u>read only memory</u> 206 and the <u>hard disk drive</u> 210" (emphasis added), all of which are computer readable mediums.

Issue # 2:

The Examiner has rejected Claims 1-2, 9-14, 21-26, and 33-37 under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement.

    Group #1: Claims 1-2, 9-14, 21-24, and 37

With respect to Claims 1-2, 9-14, 21-24, and 37 the Examiner has again asserted that "[e]ach independent claim has been amended to include at least the phrase 'tangible computer readable medium'" and that "nowhere in the specification is this phrase disclosed." Appellant again disagrees and respectfully asserts that Page 11, lines 13-15 of the specification discloses "computer program instructions that may be stored in one or more of the <u>random access memory</u> 204, the <u>read only memory</u> 206 and the <u>hard disk drive</u> 210" (emphasis added), all of which are computer readable mediums.

Group #2: Claims 25-26 and 33-36

With respect to Claims 25-26 and 33-36, the Examiner has again asserted that "[e]ach independent claim has been amended to include at least the phrase 'tangible computer readable medium'" and that "nowhere in the specification is this phrase disclosed." Appellant again disagrees and respectfully asserts that Page 11, lines 13-15 of the specification discloses "computer program instructions that may be stored in one or more of the <u>random access memory</u> 204, the <u>read only memory</u> 206 and the <u>hard disk drive</u> 210" (emphasis added), all of which are computer readable mediums.

In the Office Action mailed 01/09/2007, the Examiner has responded to appellant's above argument by arguing that "Claims 25-26 and 33-37 purport to be apparatus claims, but appear to be lacking an essential element under 112, 2nd, to support the preamble and make them apparatus claims" (see page 5, paragraph 1 of the aforementioned Office Action). Appellant assumes that this argument by the Examiner refers to the above 35 U.S.C. 112, first paragraph rejection, which is addressed above.

<u>Issue # 3:</u>

The Examiner has rejected Claims 1-2, 9-14, 21-26, and 33-37 under 35 U.S.C. 101 as being directed towards non-statutory subject matter.

Group #1: Claims 1-2, and 9-12

With respect to Claims 1-2, and 9-12, the Examiner has argued that the "computer program product" as claimed by appellant "is just the software piece and fails to include the physical article or object as the medium which establishes the statutory category." Appellant disagrees and respectfully points out that independent Claim 1 includes "computer program product <u>embodied on a tangible computer readable medium</u>" (emphasis added), as claimed.

In addition, the Examiner has argued that Claims 1-2, and 9-12 fail to produce a useful, concrete, and tangible result in the instance when the update status of the current malware scanner matches

the update status of the previous malware scanner. Specifically, the Examiner has argued that the Examiner "has reviewed the final result achieved for each condition covered, both those actually recited and those covered and not recited" and concludes that "[i]f any [condition] fail[s] to be a useful, concrete, and tangible result, then the claims are properly rejected under 35 U.S.C. 101." The Examiner goes on to argue that "claim 1 does not produce a useful, concrete, and tangible result in the instance when the update status of the current malware scanner matches the update status of the previous malware scanner."

In addition, in the Office Action mailed 1/09/2007, the Examiner has again reiterated that "there is no useful, concrete, and tangible result when the update status of the previous scanner is the same as the update status of the current scanner" and that "[w]hen these statuses are the same the only steps being performed are reading and comparing and clearly these do not result in a useful, concrete, and tangible result."

Appellant respectfully disagrees. After careful review of 35 U.S.C. 101 and the relevant sections of the MPEP, appellant fails to find any support for the Examiner's assertion that "[i]f <u>any</u> [condition] fail[s] to be a useful, concrete, and tangible result, [whether or not recited in the claims,] then the claims are properly rejected under 35 U.S.C. 101" (emphasis added). Further, appellant respectfully asserts that the claims are not limited to a situation where "the update status of the current malware scanner matches the update status of the previous malware scanner," as noted by the Examiner, and thus a rejection based on such language is clearly improper.

Appellant again points out that independent Claim 1 does provide a useful, concrete and tangible result. For example, appellant claims, in part, "alert issuing logic operable if said update status of said current malware scanner does not match said update status of said previous malware scanner to <u>issue an update status alert</u> indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status…change logging logic <u>operable to log changes to said update status field</u> to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history…wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said <u>update</u>

status field associated with said computer file is changed to correspond to said current malware scanner… wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated" (emphasis added), as claimed. In fact, in independent Claim 1 appellant claims a "computer program product embodied on a tangible computer readable medium operable to control a computer to issue an alert for an out-of-date update status of a malware scanner" (emphasis added), as claimed, which clearly is a useful, concrete and tangible result.

Therefore, based on the limitations in Claim 1, as highlighted above, it is clear that a useful, concrete and tangible result is evident.

   Group #2: Claims 13-14 and 21-24

The Examiner has argued that Claims 13-14 and 21-24 fail to produce a useful, concrete, and tangible result in the instance when the update status of the current malware scanner matches the update status of the previous malware scanner. Specifically, the Examiner has argued that "claim 13 does not appear to produce a useful, concrete, and tangible result in the instance when the update status of the current malware scanner matches the update status of the previous malware scanner."

In addition, in the Office Action mailed 1/09/2007, the Examiner has again reiterated that "there is no useful, concrete, and tangible result when the update status of the previous scanner is the same as the update status of the current scanner" and that "[w]hen these statuses are the same the only steps being performed are reading and comparing and clearly these do not result in a useful, concrete, and tangible result."

Appellant respectfully disagrees. After careful review of 35 U.S.C. 101 and the relevant sections of the MPEP, appellant fails to find any support for the Examiner's above assertion that "[i]f any [condition] fail[s] to be a useful, concrete, and tangible result, [whether or not recited in the claims,] then the claims are properly rejected under 35 U.S.C. 101" (emphasis added). Further, appellant respectfully asserts that the claims are not limited to a situation where "the update

status of the current malware scanner matches the update status of the previous malware scanner," as noted by the Examiner, and thus a rejection based on such language is clearly improper.

Appellant additionally points out that independent Claim 13 does provide a useful, concrete and tangible result. For example, appellant claims, in part, "if said update status of said current malware scanner does not match said update status of said previous malware scanner, then issuing an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status...logging changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history...wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner... wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated" (emphasis added), as claimed. In fact, in independent Claim 13 appellant claims a "computer-implemented method performed with computer code embodied on a tangible computer readable medium, for alerting an out-of-date update status of a malware scanner" (emphasis added), as claimed, which clearly is a useful, concrete and tangible result.

Therefore, based on the limitations in Claim 13, as highlighted above, it is clear that a useful, concrete and tangible result is evident.

Group #3: Claims 25-26 and 33-36

Appellant again notes that the Examiner has argued that "Claims 25-26 and 33-37 purport to be apparatus claims, but appear to be lacking an essential element under 112, 2nd, to support the preamble and make them apparatus claims" and that "[a]s such, they appear to be merely software (functional descriptive material), per se, and non-statutory under 35 U.S.C. 101 rather than an actual apparatus." Appellant assumes that this argument by the Examiner refers to the above 35 U.S.C. 112, first paragraph rejection, which is addressed above.

Additionally, the Examiner has argued that Claims 25-26 and 33-36 fail to produce a useful, concrete, and tangible result in the instance when the update status of the current malware scanner matches the update status of the previous malware scanner. Specifically, the Examiner has argued that "[c]laim 25 also appears to have the same issue of claim 1 and claim 13 regarding the conditional nature of the final result achieved."

Further, in the Office Action mailed 1/09/2007, the Examiner has again reiterated that "there is no useful, concrete, and tangible result when the update status of the previous scanner is the same as the update status of the current scanner" and that "[w]hen these statuses are the same the only steps being performed are reading and comparing and clearly these do not result in a useful, concrete, and tangible result."

Appellant respectfully disagrees. After careful review of 35 U.S.C. 101 and the relevant sections of the MPEP, appellant fails to find any support for the Examiner's above assertion that "[i]f <u>any</u> [condition] fail[s] to be a useful, concrete, and tangible result, [whether or not recited in the claims,] then the claims are properly rejected under 35 U.S.C. 101" (emphasis added). Further, appellant respectfully asserts that the claims are not limited to a situation where "the update status of the current malware scanner matches the update status of the previous malware scanner," as noted by the Examiner, and thus a rejection based on such language is clearly improper.

Appellant additionally points out that independent Claim 25 does provide a useful, concrete and tangible result. For example, appellant claims, in part, "an alert issuer operable if said update status of said current malware scanner does not match said update status of said previous malware scanner to <u>issue an update status alert</u> indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status…a change logger operable to <u>log changes to said update status field</u> to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history…wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said <u>update status field associated with said computer file is changed</u> to correspond to said

current malware scanner... wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated" (emphasis added), as claimed. In fact, in independent Claim 25 appellant claims an "[a]pparatus including a tangible computer readable medium for issuing an alert for an out-of-date update status of a malware scanner" (emphasis added), as claimed, which clearly is a useful, concrete and tangible result.

Therefore, based on the limitations in Claim 25, as highlighted above, it is clear that a useful, concrete and tangible result is evident.

Group #4: Claim 37

Appellant notes that the Examiner has argued that "[Claim]... 37 purport[s] to be [an] apparatus [claim], but appear[s] to be lacking an essential element under 112, 2nd, to support the preamble and make [Claim 37 an] apparatus [claim]" and that "[a]s such, [Claim 37] appear[s] to be merely software (functional descriptive material), per se, and non-statutory under 35 U.S.C. 101 rather than an actual apparatus."

Appellant respectfully asserts that Claim 37 clearly claims "[a] computer program product as claimed in claim 1, wherein said update status alert triggers an automatic update to said malware scanner in accordance with one of administrator preferences and user preferences" (emphasis added), as claimed, and clearly does not "purport to be [an] apparatus [claim]," as stated by the Examiner above.

Furthermore, appellant respectfully asserts that in Claim 37, as dependent upon independent Claim 1, a useful, concrete and tangible result is evident for the reasons argued with respect to independent Claim 1 in Issue #3, Group #1.

In view of the remarks set forth hereinabove, all of the independent claims are deemed allowable, along with any claims depending therefrom.

VIII CLAIMS APPENDIX (37 C.F.R. § 41.37(c)(1)(viii))

The text of the claims involved in the appeal (along with associated status information) is set forth below:

1. (Previously Presented) A computer program product embodied on a tangible computer readable medium operable to control a computer to issue an alert for an out-of-date update status of a malware scanner, said computer program product comprising:

(i) reading logic operable to read an update status field associated with a computer file to be scanned by a current malware scanner, said update status field being indicative of an update status of a previous malware scanner that has scanned said computer file and associated said update status field with said computer file;

(ii) comparison logic operable to compare said update status of said previous malware scanner with an update status of said current malware scanner;

(iii) alert issuing logic operable if said update status of said current malware scanner does not match said update status of said previous malware scanner to issue an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

(iv) change logging logic operable to log changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history;

wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner;

wherein said update status alert includes one or more of:

(i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated;

wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners;

wherein said update status file and said computer file are combined into a combined file that is passed as a single entity between said malware scanners;

wherein said combined file is a file compressed combination of said update status file and said computer file.

2. (Original) A computer program product as claimed in claim 1, wherein said update status field is included as a property field within said computer file.

3. – 8. (Cancelled)

9. (Original) A computer program product as claimed in claim 1, wherein said computer file is an e-mail attachment.

10. (Original) A computer program product as claimed in claim 1, wherein said current malware scanner and said previous malware scanner are part of a tiered malware scanner.

11. (Original) A computer program product as claimed in claim 1, wherein said update status field includes one or more of:

    (i) a malware scanner computer program product identifier;

    (ii) a computer hardware identifier;

    (iii) a scanner engine program version identifier; and

    (iv) a malware definition data version identifier.

12. (Previously Presented) A computer program product as claimed in claim 1, wherein said malware scanner serves to detect one or more of:

    (i) a computer virus;

    (ii) a Trojan computer program;

    (iii) a worm computer program;

    (iv) a banned computer program; and

(v) banned content within a e-mail.

13. (Previously Presented) A computer-implemented method performed with computer code embodied on a tangible computer readable medium, for alerting an out-of-date update status of a malware scanner, said method comprising:

reading an update status field associated with a computer file to be scanned by a current malware scanner, said update status field being indicative of an update status of a previous malware scanner that has scanned said computer file and associated said update status field with said computer file;

comparing said update status of said previous malware scanner with an update status of said current malware scanner;

if said update status of said current malware scanner does not match said update status of said previous malware scanner, then issuing an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

logging changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history;

wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner;

wherein said update status alert includes one or more of:

(i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated;

wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners;

wherein said update status file and said computer file are combined into a combined file that is passed as a single entity between said malware scanners;

wherein said combined file is a file compressed combination of said update status file and said computer file.

14. (Original) A method as claimed in claim 13, wherein said update status field is included as a property field within said computer file.

15. – 20. (Cancelled)

21. (Original) A method as claimed in claim 13, wherein said computer file is an e-mail attachment.

22. (Original) A method as claimed in claim 13, wherein said current malware scanner and said previous malware scanner are part of a tiered malware scanner.

23. (Original) A method as claimed in claim 13, wherein said update status field includes one or more of:

(i) a malware scanner computer program product identifier;

(ii) a computer hardware identifier;

(iii) a scanner engine program version identifier; and

(iv) a malware definition data version identifier.

24. (Previously Presented) A method as claimed in claim 13, wherein said malware scanner serves to detect one or more of:

(i) a computer virus;

(ii) a Trojan computer program;

(iii) a worm computer program;

(iv) a banned computer program; and

(v) banned content within a e-mail.

25. (Previously Presented) Apparatus including a tangible computer readable medium for issuing an alert for an out-of-date update status of a malware scanner, said apparatus comprising:

(i) a reader operable to read an update status field associated with a computer file to be scanned by a current malware scanner, said update status field being indicative of an update status of a previous malware scanner that has scanned said computer file and associated said update status field with said computer file;

(ii) a comparitor operable to compare said update status of said previous malware scanner with an update status of said current malware scanner;

(iii) an alert issuer operable if said update status of said current malware scanner does not match said update status of said previous malware scanner to issue an update status alert indicative of an out-of-date update status for whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(iv) a change logger operable to log changes to said update status field to create a change history in an update status tracking database to enable identification of weaknesses within update status management based on the change history;

wherein, if said current malware scanner has a less out-of-date update status than said previous malware scanner, then said update status field associated with said computer file is changed to correspond to said current malware scanner;

wherein said update status alert includes one or more of:

(i) a user alert issued on whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status; and

(ii) an administrator alert issued to an administrator of whichever one of said current malware scanner and said previous malware scanner has a most out-of-date update status;

wherein, if there is no said update status associated with said computer file at a first malware scanning, then said update status field is generated and associated with said computer file, and said update status tracking database is updated;

wherein said update status field is included within an update status file passed together and associated with said computer file between malware scanners;

wherein said update status file and said computer file are combined into a combined file that is passed as a single entity between said malware scanners;

wherein said combined file is a file compressed combination of said update status file and said computer file.

26. (Original) Apparatus as claimed in claim 25, wherein said update status field is included as a property field within said computer file.

27. – 32. (Cancelled)

33. (Original) Apparatus as claimed in claim 25, wherein said computer file is an e-mail attachment.

34. (Original) Apparatus as claimed in claim 25, wherein said current malware scanner and said previous malware scanner are part of a tiered malware scanner.

35. (Original) Apparatus as claimed in claim 25, wherein said update status field includes one or more of:

      (i) a malware scanner computer program product identifier;

      (ii) a computer hardware identifier;

      (iii) a scanner engine program version identifier; and

      (iv) a malware definition data version identifier.

36. (Previously Presented) Apparatus as claimed in claim 25, wherein said malware scanner serves to detect one or more of:

      (i) a computer virus;

      (ii) a Trojan computer program;

      (iii) a worm computer program;

      (iv) a banned computer program; and

      (v) banned content within a e-mail.

37. (Previously Presented) A computer program product as claimed in claim 1, wherein said update status alert triggers an automatic update to said malware scanner in accordance with one of administrator preferences and user preferences.

IX EVIDENCE APPENDIX (37 C.F.R. § 41.37(c)(1)(ix))

There is no such evidence.

X RELATED PROCEEDING APPENDIX (37 C.F.R. § 41.37(c)(1)(x))

N/A

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 971-2573. For payment of any additional fees due in connection with the filing of this paper, the Commissioner is authorized to charge such fees to Deposit Account No. 50-1351 (Order No. NAI1P495).

Respectfully submitted,

By: ___/KEVINZILKA/_____   Date: _____November 19, 2008_____
Kevin J. Zilka
Reg. No. 41,429

Zilka-Kotab, P.C.
P.O. Box 721120
San Jose, California 95172-1120
Telephone: (408) 971-2573
Facsimile: (408) 971-4660